(U//FOUO) IRANIAN CYBER ACTOR CRITICAL TARGETING CAMPAIGN AGAINST PLC DEVICES

(U//FOUO) Iranian cyber actors have placed an increased emphasis on the immediate identification and exploitation of Programmable Logic Controllers. This is likely a direct response to the ongoing hostilities between Iran and the U.S. and critical allies. The following information is being shared to solidify the defensive posture of industry partners who may operate these PLC devices. This is being shared in anticipation of Iranian intent to support destructive actions should they succeed in exploitation efforts.

(U//FOUO) Ongoing Iranian PLC Campaign

(U//FOUO) Iranian actors have placed emphasis on the exploitation of PLC devices in order to hold infrastructure at risk in support of their operational objectives during the ongoing crisis. The intent of this exploitation is presumed to be support to Iranian destructive operations. Iranian actors have been noted prioritizing the identification, exploitation, and presumed destructive targeting of the following device types:

- **(U//FOUO) Rockwell Automation CompactLogix 5370 Series** (1769-L series including L16ER, L18ER, L19ER, L24ER, L30ER, L33ER, L36ERM variants)

- **(U//FOUO) Rockwell Automation Micro850 Series** (2080-L50E variants)

(U//FOUO) These devices have been noted playing a key role in the Critical Infrastructure and Key Resources (CIKR) operational environment. The utilization by a large number of key municipalities with varying levels of cyber security has served to significantly raise the threat profile of these actors and necessitate this unique notice. The above list is not expected to be an exhaustive coverage of the current campaign, and other devices types may be included in the current cyber operation. It is unclear what attack vector the actors may be leveraging to facilitate their current operations and it is possible they are leveraging non-public exploitation approaches. Given the unknown operation attack vector, the following CVEs could possibly be utilized to support any potential operations.

- (U//FOUO) CVE-2022-1159 & CVE-2022-1161 (CVSS 10.0 - Critical): Unauthenticated remote code execution via Common Industrial Protocol (CIP). Attackers can achieve complete controller compromise, modify ladder logic, cause denial of service, or exfiltrate operational data without any authentication.

- (U//FOUO) CVE-2021-22681 (CVSS 10.0 - Critical): Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to bypass the verification mechanism and connect with Logix controllers.

- (U//FOUO) CVE-2019-10954 (CVSS 7.5): Denial of service vulnerability allowing malformed CIP packets to crash controllers and disrupt operations.

(U//FOUO) Mitigating the Iranian PLC Threat to Highlighted PLCs

(U//FOUO) The severity of the threat posed by Iranian actors in the current operating environment is high, and prioritization of identifying and hardening devices that may be targeted in this current campaign is strongly recommended. Operators with targeted devices should consider working with the vendor and/or managed service providers to address specific threats. The following information is provided to aide operators with the affected devices in understanding how to prioritize the threat.

- (U//FOUO) Prioritize systems running firmware versions 20.x, 22.x, and 30.x identified in threat intelligence.

- (U//FOUO) Scrutinize any PLCs that are directly accessible from the internet.
    - Audit firewall rules for any exposed CIP services (TCP/UDP port 44818, TCP port 2222).

- (U//FOUO) Devices that may have broad access restrictions in place are of particular interest to Iranian cyber actors.
    - (U//FOUO) Systems that did not restrict access to RSLogix 5000/Studio Logix Designer 5000 or Connected Components Workbench/FactoryTalk Design Workbench on authorized engineering workstations.
    - (U//FOUO) Systems that did not implement application whitelisting on engineering stations.
    - (U//FOUO) Systems that did not enable multi-factor authentication for all remote access to industrial control systems.

(U//FOUO) PLC Best Practices

(U//FOUO) In an effort to prevent the operational targeting of PLC devices and potential destructive operations, the following guiding principles should be implemented:

- (U//FOUO) Implement industrial DMZ architecture if not already in place.

- (U//FOUO) Enable comprehensive logging and monitoring:
    - (U//FOUO) Monitor for unauthorized configuration changes.
    - (U//FOUO) Alert on unexpected CIP traffic patterns.
    - (U//FOUO) Log all connections to PLCs.

- (U//FOUO) Implement CIP security features (if available on your firmware version):
    - (U//FOUO) Enable controller-level passwords.
    - (U//FOUO) Configure access restrictions by IP address.
    - (U//FOUO) Disable unused communication services.

- (U//FOUO) Upload project files from all controllers and store the files offline for disaster recovery.

- (U//FOUO) Refer to the following Rockwell Automation publications concerning implementing security features in the Micro850 Controllers and CompactLogix 5370 Controllers:
    - https://literature.rockwellautomation.com/idc/groups/literature/documents/um/2080-um002_-en-e.pdf (Chapter 11)
    - https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/secure-rm001_-en-p.pdf
    - https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf
    - https://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm015_-en-p.pdf

(U) Contact

(U) For information on the devices, contact Rockwell Product Security Incident Response Team (PSIRT@rockwellautomation.com)